UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED THE ACCOUNT USING INSTAGRAM USERNAME "gasgangksmith"	)	Case No. 21-mj-1193-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. s 1951	Sex trafficking by force; Sex trafficking of a minor

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Special Agent Glenn Booth

Applicant's signature

Special Agent Glenn Booth

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/18/2021 (11:04 a.m.)

/s/ The Honorable Richard A. Lloret

Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret

Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH CERTAIN GOOGLE EMAIL ACCOUNTS	)	Case No. 21-mj-1193-2

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment C

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment D

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. s 1951	Sex trafficking by force; Sex trafficking of a minor

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Special Agent Glenn Booth

Applicant's signature

Special Agent Glenn Booth

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/18/2021 (11:04 a.m.)

/s/ The Honorable Richard A. Lloret

Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret

Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH CERTAIN APPLE ICLOUD ACCOUNTS	)	Case No. 21-mj-1193-3

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment E

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment F

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. s 1951	Sex trafficking by force; Sex trafficking of a minor

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Special Agent Glenn Booth

Applicant's signature

Special Agent Glenn Booth

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/18/2021 (11:04 a.m.)

/s/ The Honorable Richard A. Lloret

Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret

Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE (215)-303-0543, WITH SERVICE PROVIDED BY T-MOBILE	)	Case No. 21-mj-1193-4

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment G

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment H

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. s 1951	Sex trafficking by force; Sex trafficking of a minor

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Special Agent Glenn Booth

Applicant's signature

Special Agent Glenn Booth

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/18/2021 (11:04 a.m.)

/s/ The Honorable Richard A. Lloret

Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH THE INSTAGRAM ACCOUNT USING USERNAME "gasgangksmith"	)	Case No. 21-mj-1193-1

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate.

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 08/18/2021 11:04 am

/s/ The Honorable Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret
Printed name and title

Return

Case No.: 21-mj-1193-1	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	
INFORMATION ASSOCIATED WITH CERTAIN GOOGLE EMAIL ACCOUNTS	)	Case No. 21-mj-1193-2

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment C

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment D

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate.

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 08/18/2021 11:04 am

/s/ The Honorable Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 21-mj-1193-2	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH CERTAIN APPLE ICLOUD ACCOUNTS	)	Case No. 21-mj-1193-3

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment E

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment F

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate.

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 08/18/2021 11:04 am

/s/ The Honorable Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 21-mj-1193-3	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE (215)-303-0543, WITH SERVICE PROVIDED BY T-MOBILE.	)	Case No. 21-mj-1193-4

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment G

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment H

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate.

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 08/18/2021 11:04 am

/s/ The Honorable Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

The Honorable Richard A. Lloret
Printed name and title

Return

Case No.: 21-mj-1193-4	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH VARIOUS ELECTRONIC ACCOUNTS	Case No. 21-mj-1193 **Filed Under Seal**

CONSOLIDATED AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANTS

I, Glenn G. Booth, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit to apply for warrants to search the following electronic accounts[1]:

- **Target Account 1**: The Instagram account using username "gasgangksmith," believed to be used by Kevin SMITH (Attachments A-B);
- **Target Account 2**: The Google e-mail ("g-mail") account address "kevinsmith589@gmail.com," believed to be used by Kevin SMITH (Attachments C-D);
- **Target Account 3**: The Google e-mail ("g-mail") account address "khajirsmith1787@gmail.com," believed to be used by Kevin SMITH (Attachments C-D);
- **Target Account 4**: The Apple I-Cloud account associated with "khajirsmith1787@gmail.com" and "imselfmade8989@icloud.com," believed to be used by Kevin SMITH (Attachments E-F);
- **Target Account 5**: The cellular telephone assigned number (215)-303-0543, with service provided by T-Mobile, believed to be used by Kevin SMITH (Attachments G-H).

(herein the "**Target Accounts**").

2. The warrants would authorize the search of the **Target Accounts** for the information described the following paragraphs and in Attachments A, C, E and G, and would require Facebook, Inc. (which owns Instagram) Google LLC, Apple, Inc., and T-Mobile (herein

[1] I apply for such authority under Federal Rule of Criminal Procedure 41, Title 18 of the United States Code Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A).

"the PROVIDERS") to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B, D, F, and H. Upon receipt of the information described in Section I of Attachments B, D, F, and H, government-authorized persons will review that information to locate the items described in Section II of Attachments B, D, F, and H, using the procedures described in Section III of those Attachments.

AGENT BACKGROUND

3. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been employed as a Special Agent of the FBI for over twenty-three years, and am currently assigned to the Philadelphia Division, Fort Washington Resident Agency, where I investigate various matters including Violent Crimes Against Children. During my career, I have worked cases involving but not limited to Sex Trafficking, Child Sex Trafficking and Child Pornography. I have also worked dozens of cases involving the use of the internet and social media to perpetrate crimes such as Violent Crimes Against Children and Child Sex Trafficking. I have gained experience through my participation in these cases and through training at the FBI Academy, numerous conferences, and online training courses. I have also presented case studies regarding Child Sex Trafficking at regional and national conferences.

4. In my training and experience, criminals who manage sex trafficking enterprises frequently use violence, intimidation, and physical force to run their affairs. These sex traffickers sometimes use force to protect their victims from threats posed by customers, but also often use violence to force women or girls to remain working for them conducting commercial sex. I am also aware, from my training and experience, that sex traffickers frequently manipulate and abuse—both physically and emotionally—women in order to force them to engage in prostitution, and exploit women sexually and financially for themselves. Relatedly, sex traffickers frequently

target vulnerable women, including drug addicts, juveniles, and other distressed or troubled females, to entice them to engage in commercial sex on their behalf. I am also aware that sex traffickers often provide women with controlled substances in order to foster their attachment (via addiction) to the sex trafficker as well as the sex trafficking enterprise.

5. Based on my training and experience working sex trafficking cases, I am aware that criminals who profit from the sex trafficking of women and children in violation of federal law frequently use digital user accounts, including e-mail address accounts, social media accounts, and Internet websites, to further their activities. For example, sex traffickers frequently use Internet websites to advertise the sexual services of their victims. These websites include Craig's List, Backpage.com,[2] Escort Fish, MegaPersonals, and other sites that allow classified or anonymous advertisements of this nature. I am also aware, from my training and experience, that users must set up accounts to post such advertisements that are linked to an electronic mail account ("e-mail address").

6. Accordingly, a search of e-mail accounts used to post online sex advertisements can discover valuable evidence of sex trafficking, including information about (i) the site and internet address used to advertise sexual services; (ii) the identity of the individual or entity who posted the advertisement; (iii) the identity and background of the victim; (iv) the content, including any message, images, captions, or other attachments, of the advertisement; (v) any responses, messages, or other communications from individuals who respond to the advertisement and solicit the sexual services; (vi) metadata, transactional data, and background information regarding the date, time, and content of the advertisement; (vii) the method and means of communication used

[2] This website is now defunct.

by sex traffickers for subsequent contacts and arrangements between customers and sex trafficked workers; and (viii) other relevant evidence of illegal sex trafficking.

7. Similarly, I am also aware that the invention of "smart phones" (e.g. Apple iPhones and Samsung Galaxy) has also developed the means by which sex traffickers can conduct criminal activity. Through the use of mobile "smart" phones, sex traffickers can now directly access the Internet from their phone and conduct sex trafficking activity therefrom by (i) posting online advertisements of their victims; (ii) communicating with their victims, sex buyers, and coconspirators through all sorts of mobile communication applications, including social media; (iii) taking pictures and videos of sex trafficking victims to advertise their services; (iv) accessing their e-mail accounts to coordinate and conduct sex trafficking business; (v) accessing other internet websites in furtherance of sex trafficking activity; (vi) and other uses. Accordingly, a search of smart phones, as well as their remote digital back-ups maintained by the phone manufacturer (i.e. an Apple I-Cloud account) can reveal valuable evidence of these criminal activities.

8. My training and experience also indicates that sex traffickers have increasingly used social media accounts to further their criminal activity. Specifically, these criminals use social media accounts to (i) entice and solicit women and minors to join their sex trafficking enterprise, (ii) communicate with sex trafficking victims in the normal course of their business; and (iii) otherwise conduct their illegal sex trafficking business with potential customers. Accordingly, a search of these social media accounts can likewise find valuable evidence of sex trafficking, including information regarding (i) the identity of individuals engaged in sex trafficking; (ii) the identity of, and communications between sex buyers, coconspirators, employees, and victims; (iii) images, videos, direct messages, and other content that is relevant

evidence of sex trafficking business; (iv) location information of the user and their criminal activity; (iv) other contact information (i.e. phone numbers, e-mail accounts, IP addresses) of individuals engaged in sex trafficking.

9. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

PROBABLE CAUSE

10. The Federal Bureau of Investigation as well as state and local law enforcement have been investigating Kevin SMITH (DOB: 07/14/1994) for several years for a sex trafficking enterprise he has conducted from on or around July 31, 2015 to October 1, 2019 using actual or threatened physical force and violence, and which has involved minors. As detailed below, there is probable cause that SMITH has violated Title 18, United States Code, Section 1591 (sex trafficking of minors and sex trafficking by force), and that a search of the **Target Accounts** will reveal evidence of those crimes. As described below, both confidential witnesses and law enforcement officers relate that SMITH has run an illegal sex trafficking enterprise that has involved violence and underage girls.

Law Enforcement Arrests and Interviews (2015-2018)

11. On September 4, 2015, Bensalem Police Department officers responded to a call for a violent domestic disturbance at the Quality Inn Hotel at 3671 Street Road, Bensalem, Pennsylvania to find a Confidential Witness ("CW1") visibly beaten with "several ligature marks around her neck" and "bruises on her left arm." When interviewed, CW1 told officers she prostituted for her "pimp" SMITH for the past two-and-a-half months during which SMITH would

post online advertisements (including on Backpage.com) for interested sex buyers to have sex with CW1 for money. CW1 related that SMITH would retain all proceeds from the commercial sex acts (up to $1,000 a day) and effectively forced her to work for free save for taking care of her expenses. In fact, CW1 stated that SMITH physically assaulted her because on this occasion CW1 protested the work conditions and attempted to keep the money for her own. Enraged, SMITH grabbed CW1 by the throat and choked her to the point of losing consciousness. He then threw her across the room and slammed her head on a mattress, causing her glasses to break and lacerating her beneath her left eye. After the incident, SMITH seized the proceeds of CW1's sex acts that night ($800) and left. CW1 provided a signed statement back at the police station and photographs were taken of her injuries.

12. On November 9, 2016, undercover officers with the Bensalem Police Department responded to an advertisement for sexual services by a minor CW4 (DOB: 07/xx/1999) at the Radisson Hotel, and found CW4 in a hotel room (430) rented out by and registered in the name of CW1. Investigators subsequently found CW1 in another room (649) in the hotel she had rented. CW4 did not cooperate with law enforcement regarding the underlying sex trafficking scheme, but did admit to engaging in prostitution in the past. She was arrested for prostitution.

13. A week later, investigators once more interviewed CW4. On this occasion, November 14, 2016, investigators tried to have CW4 identify her "pimp," but CW4 claimed that she was working on her own. Both federal and state law enforcement believe CW4 was attempting to protect SMITH from criminal liability. Nevertheless, when pressed, CW4 did admit that SMITH was engaged in illegal sex trafficking, and—most notably—admitted that she had worked for SMITH years ago underage (she was even still a minor at the time of this interview). She further stated that she had prostituted at numerous hotels in Bensalem Township and Bristol

Township during this time with both CW1 and SMITH. Investigators requested to search CW4's phone, at which point she stated that they would find text messages to SMITH involving giving him money, and that CW1 had given her the phone. While she denied working for SMITH and CW1 during this time, based on my investigation and these admissions by CW4, I believe that CW4 was performing sex work for SMITH's sex trafficking enterprise during this period.

14. On June 26, 2017, Philadelphia Police Department officers responded to a report of a violent assault at or around 6144 Pine Street, Philadelphia, Pennsylvania. Upon arrival, officers observed visible injuries (bruise under eye, scratch marks/bruises on neck) on CW1, who reported that SMITH had struck her in the face multiple times with a closed fist and choked her.

15. A few days later, on June 30, 2017, Tinicum Township Police Department officers responded to another call for a violent assault committed by SMITH on CW1 at the Wyndham Gardens Hotel, Room 452, at 45 Industrial Highway, Essington, Pennsylvania. When officers arrived, medical personnel were already treating CW1 for her injuries—including visible facial injuries as well as body trauma. Officers interviewed CW1, who reported that SMITH forcibly entered her hotel room and immediately attacked her with punches to the face and kicks to her body. SMITH proceeded to choke CW1 until she was unconscious, and then fled when an eyewitness saw the violent assault and called police.

16. In the aftermath of law enforcement responding to the scene, and during their interview of CW1, SMITH called CW1 on her cell phone repeatedly. CW1 answered her phone at one point, and one of the police officers overheard a male (believed to be SMITH) stating that he did not kick her in the face, and only punched her in the face.

Witness Statements

17. CW1 has been interviewed by law enforcement several times[3] in relation to SMITH's sex trafficking enterprise. To my knowledge, CW1 has not cooperated in the hopes of leniency on pending charges. She has, however, at times minimized her own role and that of SMITH in the sex trafficking business, including in an interview on January 21, 2017 where she omitted much of the illegal acts committed by SMITH that are discussed in this affidavit. However, she would later state in her July 25, 2017 interview that she was afraid that SMITH would direct violence against her if she cooperated against him.

18. To summarize the content of these interviews, CW1 functioned as the "bottom" (i.e. a trusted subordinate/deputy who would assume some tasks of running the sex trafficking enterprise) for SMITH during an extensive period of his sex trafficking, and she related that SMITH conducted a sex trafficking ring from the time she met him (July 31, 2015) until her last contact with him in or around the summer of 2017. She stated that SMITH would manage the prostitution of several (five or sex) girls at a time during this period, including underage girls such as CW4 and another minor named "Diamond" (real name unknown), and specifically recalled CW4 working for SMITH in Buck's County, Pennsylvania, in the fall of 2016. This information has been corroborated during the arrest of CW1 and CW4 on November 9, 2016, and the post-arrest interviews of CW4 that occurred afterward. CW1 claims she did not know CW4 was underage until this incident, but recollected that SMITH met CW4 on Instagram (i.e. **Target Account 1**).

[3] These interviews occurred as follows: (i) September 4, 2015 by the Bensalem Police Department in response to a 9-1-1 call for a violent assault; (ii) June 3, 2016 by the Bensalem Police Department in response to a call for a domestic disturbance; (iii) June 30, 2017, in the Taylor Hospital, 175 East Chester Pike, Ridley Park, Pennsylvania, by the Federal Bureau of Investigation after SMITH violently assaulted her; (iv) July 25, 2017 by the Federal Bureau of Investigation once CW1 was released from the hospital in the aftermath of the June 30, 2017 assault.

19. CW1 also identified "Diamond" (Name Unknown), "Shay" (Name Unknown), CW2, another underage girl named "Diamond" (Name Unknown), and other girls who worked for SMITH during this time. CW1 stated that SMITH frequently used violence to coerce women to remain in his employ and effectively work for free (he would pay expenses). CW1 recalls one incident in the spring of 2017 where SMITH punched "Diamond" in the face and broke her nose during an argument over the arrangement. CW1 specifically estimates that SMITH beat her more than fifty times, and she would "get the shit beaten out of her" anytime she questioned SMITH's relationship with other girls or the financial arrangement of the business. CW1 also recalled one incident where she did not give SMITH the money earned from prostituting: SMITH drove to pick her up under the pretense of taking her out to eat, and then beat her and left her on the side of the road. CW1 recalled another incident in or around November or December 2016, when she tried to leave him at 30th Street Station in Philadelphia, Pennsylvania. SMITH pursued her with an associate ("Jay") and physically dragged her to his car before putting a firearm to her stomach and pulling the trigger. According to CW1, the gun jammed.

20. Confidential Witness 2 ("CW2") also prostituted for SMITH and was interviewed on October 4, 2017, and October 11, 2017. CW2 claims she knew SMITH for many years and was aware that he had a sex trafficking ring during that time period, which included a minor girl ("Mxxxx") who was approximately fifteen years old at the time. CW2 relates, however, she only began to work for SMITH in early 2017 in Wilmington, Delaware. CW2 corroborated that either SMITH, herself, or another girl would post advertisements online for her sexual services, and then set up "dates" with interested sex buyers. CW2 also stated that SMITH demanded ***all*** of the money she earned from prostitution, and that SMITH would only pay her expenses, although on occasion he would provide her with marijuana or Percocet pills.

21. CW2 corroborated that SMITH violently forced women to engage in sex trafficking. She recalls one occasion, on a date she cannot remember precisely, in which SMITH slapped her in a hotel room because CW2 complained about the arrangement of her working for him for free, and therefore wanted to leave him. She stated that SMITH slapped her on multiple occasions while she prostituted for him. While on one occasions she did state that she did not "necessarily" stay with SMITH because she was afraid, on other occasions she did admit she was afraid of him, that he would not let her leave, and that he often carried firearms. CW2 also observed SMITH physically assault CW1 on multiple occasions during this period (circa early 2017 to October 2017), and that CW1 warned CW2 that SMITH was dangerous and had in fact killed people. CW2 also confirmed that SMITH used **Target Account 1** to communicate with girls who worked for him, and showed investigators some of the direct messages on Instagram between her and SMITH.

22. Confidential Witness 3 (CW3) also was prostituted by SMITH, and was interviewed on January 8, 2018 and October 5, 2018. She confirmed SMITH managed a sex trafficking enterprise in the greater Philadelphia area from 2017 to 2018 in which he would retain all revenue earned by the women, and would only provide their basic expenses for the job such as food and clothing. CW3 corroborated that CW1 and CW2 were prostituted by SMITH, and CW1 functioned as the "bottom" (previously defined) girl. CW3 claimed that SMITH managed several girls during this period (including CW1 and CW2), and that either himself or CW1 would book the hotel rooms for CW3 and other women to engage in commercial sex.

23. CW3 also detailed that SMITH would violently assault women, and recalls the aforementioned incidents in which SMITH physically assaulted both CW1 and CW2. SMITH also physically beat CW3 (breaking her nose) inside of a vehicle, she claimed, after he learned that

she was talking to another male on the phone. On another occasion while SMITH was running his sex trafficking enterprise in Delaware, he beat CW3, threw her down a flight of stairs, and then threw a firearm at her. CW3 also recalled that all women who worked for SMITH had to get tattoos of his name on their body (a claim CW1 made as well), and investigators have observed and photographed some of these tattoos. CW3 stated that, in general terms, that she felt that she could never leave SMITH out of fear of violent retaliation.

24. As noted above, CW4 (a minor) provided some limited information regarding SMITH during interviews on November 9, 2016 and November 14, 2016, although these statements did indicate, as I explain above, that she was being prostituted by SMITH during this period. While CW4 has discussed working for other sex traffickers besides SMITH in other interviews (conducted on January 3, 2016 and May 31, 2016), she has declined other attempts by law enforcement to ask her about SMITH's sex trafficking activities. However, in another interview in August 27, 2018 conducted by the FBI, CW4 claimed that SMITH approached her recently to solicit her to prostitute for him. The timing of this solicitation is not clear, and CW4 had recently turned 18 years old at the time of the interview.

Interview of Kevin Smith (January 25, 2017)

25. On January 21, 2017, the FBI interviewed SMITH under the pretense of wanting information regarding another sex trafficker named Derrick HEPPARD. SMITH agreed to the interview, during which he admitted to managing CW1 in a sex trafficking enterprise, but claimed it was consensual and equitable. While he denies ever managing minor CW4, he confessed that he put CW4 in touch with CW1 for the purposes of reentering the sex trafficking business with her.

The Sex Trafficking of Minor Confidential Witness 5

26. In late September 2019, SMITH forced a runaway minor, Confidential Witness 5 ("CW5") (DOB: 08/xx/2004), to prostitute for him for several days from roughly September 24, 2017 until September 27, 2017. After her rescue by law enforcement, investigators interviewed CW5 on October 16, 2017.

27. According to CW5 and other witness statements, she ran away from home (in Media, Pennsylvania) on September 21, 2019, and her parents reported her missing that same day. The following day, CW5 and another juvenile friend boarded a train station to Philadelphia, where they later encountered the cousin of SMITH (Confidential Witness 6 – "CW6"). According to both CW5 and CW6, CW6 let CW5 stay at a friend's house for one night before he handed her off to SMITH on the understanding that CW5 could stay with him indefinitely.

28. On or around September 23, 2019, CW6 and SMITH met in a parking lot, at which point CW5 was passed over to SMITH's care. SMITH then drove CW5 to 385 Harrison Street, Apartment B3, Upper Darby, Pennsylvania, where he forced CW5 to undress, put on undergarments SMITH provided, and pose for pictures. When CW5 questioned SMITH about this, SMITH stated that if she did not do what he said he would confiscate the clothes he loaned her and essentially put her out on the street naked and with no money or phone.

29. Repeating this same threat, SMITH then raped CW5 on the couch in the apartment. In addition to the threat of leaving her naked, penniless, and abandoned in an unknown location, CW5 thought SMITH was very "scary" and had a threatening demeanor and tone. CW5 claimed that she told SMITH to "stop" during the sex, but he refused.

30. According to CW5, SMITH then forced CW5 to have sex with men for money in the days that followed—from approximately September 23, 2019 until September 26, 2019. SMITH, according to CW5 and as corroborated by electronic evidence, posted CW5's pictures on

the internet sites "MegaPersonals" and "Escort Fish," and then—with the assistance of a coconspirator ("CC1") who also worked for SMITH—facilitated dates with men who responded to these advertisements to have sex for money. As with the other women SMITH employed, CW5 received no money and was ordered to surrender anything she earned to SMITH. CW5 stated that SMITH drove her to many of the commercial sex encounters, although another coconspirator sometimes facilitated the encounters as well.

31. CW5 does not recall how many times or for how long she was forced to perform sex for SMITH. She claims that she did so out of fear and that she did not try to escape due to a hope that if she did what SMITH said, he would eventually let her go. On or around September 28, 2019, CC1 allowed CW5 to flee from her vehicle upon learning of SMITH's arrest.

32. Towards the end of her time working for SMITH, on or around September 27, 2019, one of the sex buyers (Confidential Witness 7 ("CW7")) who responded to an advertisement for CW7 and who ultimately purchased sex from her, observed a media bulletin notifying the public of CW5's disappearance. CW7 promptly notified law enforcement, and was later interviewed on October 22, 2019 as well as May 13, 2021, by law enforcement. CW7 confirmed transacting with CW5 for sex, although he claimed he did not know she was a minor. CW7 stated that he came forward not out of fear of criminal liability, but rather due to a genuine concern for CW5's safety. CW7 also stated that CW5 was accompanied by another female, believed to be CC1, who seemed to be in charge.

33. Law enforcement officers recovered a cell phone from SMITH after his arrest, and obtained warrants to search its contents. When law enforcement obtained a warrant to search

SMITH's cell phone,[4] the evidence recovered showed that (i) the phone number associated with this device was **Target Account 5** ((215)-303-0543); (ii) the Apple I-Cloud account identifiers were **Target Account 3** and **Target Account 4**—i.e. the e-mail accounts apparently registered by SMITH for his Apple I-Cloud account; and (iii) the e-mail account associated with SMITH and is phone was **Target Account 2**. In short, a search of this cellular phone confirmed that SMITH was the user of **Target Accounts 2-5**.

34. In addition, SMITH's phone also contained the advertisements posted for the sexual services of CW5 on MegaPersonals.com, which further confirms that SMITH used this phone to conduct his sex trafficking of CW5. This phone also contained searches for CW5's name ("***** *******"), as well as reviewing articles concerning her disappearance.

THE TARGET ACCOUNTS

35. As summarized above, there is probable cause to believe that SMITH has committed violations of Title 18, United States Code, Section 1591 (sex trafficking of minors and sex trafficking by force). I further submit that there is probable cause that SMITH has used the **Target Accounts** and that a search of the **Target Accounts** will reveal evidence of a crime.[5]

36. Both CW1 and CW2 have identified SMITH as the user of **Target Account 1**, investigators have observed direct messages between SMITH and CW2 on **Target Account 1**, and CW1 indicated that SMITH first met CW4 through **Target Account 1**. A preservation order for **Target Account 1** was sent on July 7, 2021 to Facebook, Inc., for **Target Account 1**. As

[4] Investigators also determined SMITH was the user of this phone by searching the phone of his coconspirator (CC1) and noting that his phone number was named "Kev."

[5] A federal grand jury returned an indictment against Kevin SMITH last month. *See United States v. Smith*, 21-288-GEKP. However, neither this charge nor his previous arrest affects the probable cause that a search of the **Target Accounts** will reveal evidence of a crime, nor does it affect the authority for the Court to issue search warrants that can identify additional victims and crimes.

explained above regarding my general training and experience regarding sex traffickers and social media accounts, and in light of the evidence that SMITH used **Target Account 1** to communicate with his victims of sex trafficking, I submit SMITH is the user of this account and a search of it will reveal evidence of the crimes specified above.

37. CW1 has also identified SMITH as the user of **Target Account 2**, which has been corroborated by the search of SMITH's cell phone which also lists **Target Account 2** as one of his e-mail addresses. On July 13, 2017, in compliance with a Federal Grand Jury Subpoena, Backpage.com provided numerous advertisements and supporting invoices related to the email address kevinsmith689@gmail.com (i.e. **Target Account 2**). The advertisements reveal photos of girls posing both in lingerie and nude. They also include photos of CW1, CW2, and CW3. Additionally, there are photos of SMITH in a prostitution advertisement posted by a subscriber utilizing **Target Account 2**. Based on my general training and experience regarding the use of e-mail accounts to further sex trafficking activity, and in light of the statements by witnesses that SMITH regularly used Internet websites (linked with his e-mail account) to conduct sex trafficking, I submit that SMITH uses **Target Account 2** and a search of this account will reveal evidence of a crime.

38. Another e-mail account used by SMITH is **Target Account 3** as evidenced by the fact that it is listed as an Apple ID back-up on SMITH's phone, and the email address is "khajirsmith1787@gmail.com". It should also be noted that Delaware County Police detectives subpoenaed "MegaPersonals.com" for records associated with **Target Account 3**, and recovered numerous posts advertising prostitution, including the advertisements for the minor CW5 from September 23 to September 26, 2019. Accordingly, and for the reasons described above, I

submit that SMITH uses **Target Account 3** and a search of its contents will reveal evidence of a crime.

39. The search of SMITH's cell phone revealed evidence that he also has an Apple I-Cloud account linked to the e-mail addresses of **Target Account 3** and "imselfmade8989@icloud.com," i.e., **Target Account 4.** Given that SMITH's phone is indeed an Apple iPhone, it is not surprising he would have an Apple iCloud account associated with his iPhone (**Target Account 4**). As explained above and below in this affidavit, I submit that a search of **Target Account 4** will reveal evidence of SMITH's sex trafficking activity, including (i) online posts advertising sexual services of his victims, (ii) photographs and videos of victims, (iii) other mobile applications used to communicate with coconspirators, victims, and sex buyers; (iv) web activity used to further his sex trafficking enterprise; and (v) and other relevant evidence.

40. Finally, I submit that a search of **Target Account 5,** (215)-303-0543 (the number for the phone seized from SMITH), in the form of historical cell-site location information will reveal evidence of SMITH's sex trafficking of CW5 during the period of September 22-29, 2019. A search of SMITH's phone indicated he uses **Target Account 5** (i.e. that is the phone number for the device), and text messages between him and CC1 label "Kev" as the user of this phone number and also relate to the events of CW5's sex trafficking.

THE INSTAGRAM WARRANT (Target Account 1, Attachments A-B)[6]

41. Instagram is a service owned by Facebook, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510.

[6] The information in this section is based on information published by Facebook on its website and its Instagram website, including, but not limited to, the following webpages: "Data Policy,"

Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

42. Facebook collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Facebook keeps records of changes made to this information.

43. Facebook also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

44. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

45. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single

---

https://help.instagram.com/519522125107875; "Information for Law Enforcement," https://help.instagram.com/494561080557017; and "Help Center," https://help.instagram.com.

Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Facebook maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

46. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

47. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Facebook to access the contact lists on their devices to identify which contacts are Instagram users. Facebook retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Facebook to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

48. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

49. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Facebook's servers.

50. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

51. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Facebook's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

52. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

53. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the

group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

54. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

55. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Facebook retains records of a user's search history and followed hashtags.

56. Facebook collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Facebook to personalize and target advertisements.

57. Facebook uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Facebook maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and

advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

58. In some cases, Instagram users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

59. For each Instagram user, Facebook collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

60. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. As described above, the particular evidence contained on the accounts of sex traffickers can consist of all types of aspects of the sex trafficking business.

61. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Facebook can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, [[email and messaging

logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time)]] may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

62. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

63. Other information connected to the use of Instagram may lead to the discovery of additional evidence. Emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

64. Therefore, Facebook's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

THE "G-MAIL" WARRANTS (Target Accounts 2 and 3, Attachments C-D)

65. In my training and experience, I have learned that Google, LLC provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows

subscribers to obtain email accounts at the domain name "gmail.com," like the email accounts listed in Attachment C. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

66. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

67. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

68. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

69. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

70. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

THE APPLE I-CLOUD WARRANT (Target Account 4 and Attachments E-F)[7]

71. As noted above, a search of SMITH's I-Cloud account will reveal evidence of his sex trafficking activities in the form of stored communications, images, videos, contacts, other

[7] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available

accounts, location information, and other evidence. In this case, although law enforcement have obtained access to one of SMITH's phone, a search of the I-Cloud account (**Target Account 4**) may provide investigators some of the content that was no longer stored on that device, or which were stored on other electronic devices used by SMITH.

72. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

73. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email

---

at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be

purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

74. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

75. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

76. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

77. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

78. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

79. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

80. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often

created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. For sex traffickers, this data can include the identities of victims, customers, coconspirators, as well as pictures, images, and location data regarding the sex trafficking activity.

81. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

82. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

83. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or

services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

84. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

WARRANT FOR HISTORICAL CELL SITE INFORMATION (Target Account 5 and Attachments G-H)

85. In addition to applying for a warrant to search the above accounts, and incorporating the same probable cause set forth above, I also submit this affidavit for a warrant for information associated with **Target Account 5**—specifically historical cell site information relating to SMITH's involvement in the sex trafficking from September 22, 2019 until on or around September 29, 2019. This information can be valuable to locate SMITH's movements and seize evidence regarding the sex trafficking of CW5 during this period, including the locations of the commercial sex acts that CW5 was forced to undertake during this period. I have learned that T-Mobile retains cell site information for a period of 24 months such that the sought information should still be available.

86. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data

identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

87. Based on my training and experience, I know that T-Mobile can collect cell-site data about **Target Account 5**. I also know that wireless providers such as T-Mobile typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

88. Based on my training and experience, I know that wireless providers such as T-Mobile typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as T-Mobile typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because

the information can be used to identify the **Target Account 5**'s user or users and may assist in the identification of co-conspirators and/or victims.

89. In this case, historical location information concerning SMITH's phone (i.e. the **Target Account 5**) can provide valuable evidence of potential dwellings, houses, meeting places for sex trafficking, locations of coconspirators, and other relevant information related to the sex trafficking of CW5. It also, specifically, can show that he was indeed the individual who traveled to conduct the sex trafficking of CW5 and, by extension, show where he may have taken CW5 to during the course of this sex trafficking enterprise.

CONCLUSION

90. Based on the forgoing, I request that the Court issue the proposed search warrants.

91. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Facebook, Google, Apple, and T-Mobile. Because the warrant will be served on these providers, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

92. I further request that the Court direct (i) Facebook (Instagram) to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control; (ii) Google to disclose to the government any information described in Section I of Attachment D that is within its possession, custody, or control; (iii) Apple to disclose to the government any information described in Section I of Attachment F that is within its possession, custody, or control; and (iv) T-Mobile to the government any information described in Section I of Attachment H that is within its possession, custody, or control.

Respectfully Submitted,

/s/ *Glenn Booth*
Special Agent Glenn Booth
Federal Bureau of Investigation

Subscribed and sworn to before me on August 18, 2021 (11:04 a.m.)

/s/ The Honorable Richard A. Lloret
HONORABLE RICHARD A. LLORET
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A (Facebook/Instagram)

Property to Be Searched

This warrant applies to information associated with:

- The account using Instagram username "gasgangksmith" believed to be used by Kevin SMITH (**Target Account 1**);

stored at premises owned, maintained, controlled, or operated by Facebook, Inc., a company headquartered at 1601 Willow Road, Menlo Park, California.

ATTACHMENT B (Facebook/Instagram)

Particular Things to be Seized

I. Information to be disclosed by Facebook, Inc. ("Facebook")

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Facebook, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on July 7, 2021, Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the **Target Account 1**, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from July 31, 2015 until October 1, 2019**;**

7. Privacy and account settings, including change history; and

8. Communications between Facebook and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the **Target Account 1**), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from July 31, 2015 until October 1, 2019;

C. All content, records, and other information relating to communications sent from or received by the **Target Account 1** from July 31, 2015 until October 1, 2019, including but not limited to:

1. The content of all communications sent from or received by the **Target Account 1**, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the **Target Account 1**, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the **Target Account 1** and other Instagram users from July 31, 2015 until October 1, 2019 including but not limited to:

1. Interactions by other Instagram users with the **Target Account 1** or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the **Target Account 1** from July 31, 2015 until October 1, 2019; and

F. All location information, including location history, login activity, information geotags, and related metadata from July 31, 2015 until October 1, 2019..

II. Information to be Seized

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1591 those violations involving Kevin Smith and occurring after July 31, 2015 including, for each account or identifier listed on Attachment E, information pertaining to the following matters:

(a) Any and all acts of sex trafficking by force or involving minors, including online advertisements for sexual services of trafficking victims, communications between Kevin Smith and customers, victims, and coconspirators, images and videos of sex trafficking victims and the relevant sex trafficking enterprise, financial transactions and other electronic records relevant to the sex trafficking enterprise;

(b) Evidence indicating how and when the electronic account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Facebook is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

ATTACHMENT C (Google "g-mail" Accounts)

Property to Be Searched

This warrant applies to information associated with:

- **Target Account 2**: The Google e-mail ("g-mail") account address "kevinsmith589@gmail.com," believed to be used by Kevin SMITH (Attachments C-D);
- **Target Account 3**: The Google e-mail ("g-mail") account address "khajirsmith1787@gmail.com," believed to be used by Kevin SMITH (Attachments C-D);

that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT D (Google "g-mail" accounts)

Particular Things to be Seized

I. Information to be disclosed by Google LLC

To the extent that the information described in Attachment C is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment C:

a. The contents of all emails associated with the account from July 31, 2015 until October 1, 2019, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within **fourteen days** of issuance of this warrant.

II. Information to be Seized

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 of the United States Code 1591 those violations involving Kevin Smith and occurring after July 31, 2015 including, for each account or identifier listed on Attachment C, information pertaining to the following matters:

(a) Any and all acts of sex trafficking by force or involving minors, including online advertisements for sexual services of trafficking victims, communications between Kevin Smith and customers, victims, and coconspirators, images and videos of sex trafficking victims and the relevant sex trafficking enterprise, and financial transactions and other electronic records relevant to the sex trafficking enterprise;

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT E

Property to Be Searched

This warrant applies to information associated with "khajirsmith1787@gmail.com" or "imselfmade8989@icloud.com" that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT F

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment E is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment E:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account July 31, 2015 until October 1, 2019, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from July 31, 2015 until October 1, 2019, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1591 those violations involving Kevin Smith and occurring after July 31, 2015 including, for each account or identifier listed on Attachment E, information pertaining to the following matters:

(e) Any and all acts of sex trafficking by force or involving minors, including online advertisements for sexual services of trafficking victims, communications between Kevin Smith and customers, victims, and coconspirators, images and

videos of sex trafficking victims and the relevant sex trafficking enterprise, financial transactions and other electronic records relevant to the sex trafficking enterprise;

(f) Evidence indicating how and when the I-Cloud account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

ATTACHMENT G (Historical Cell Site Information)

Property to Be Searched

This warrant applies to records and information associated with:

- **Target Account 5**: The cellular telephone assigned number (215)-303-0543, with service provided by T-Mobile.

that is stored at premises controlled by T-Mobile, a wireless telephone service provider

headquartered at 3618 Factoria Boulevard, Bellevue, WA 98006.

ATTACHMENT H (Historical Cell Site Information)

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment E is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment G for the time period from September 22, 2019 until September 29, 2019:

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18 of the United States Code 1591 by SMITH during the period from September 22 to September 29, 2019.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant